

DMA Domáci úkol č. 3A

Tento úkol vypracujte a pak přineste na cvičení č. 4.

1. Nechť $n \in \mathbb{N}$. Dokažte, že
jestliže $a, b \in \mathbb{Z}$ splňují $a \equiv b \pmod{n}$, pak $13a \equiv 13b \pmod{n}$.
2. Nechť $n \in \mathbb{N}$. Dokažte, že
jestliže $a, b, c \in \mathbb{Z}$ splňují $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak $a \equiv c \pmod{n}$.

Zkouškový speciál výpočetní (doporučeno):

- a) Vypočítejte tento výraz modulo 13, použijte malou Fermatovu větu: $(7 + 8)^{146} - 21$.
- b) Najděte inverzní prvek k $a = 13$ modulo $n = 20$.

Zkouškový speciál důkazový (pokročilejší mohou zkusit teď nebo před zkouškou):

Příklady a) až c) jsou rutinní.

- a) Nechť $n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$. Dokažte, že jestliže $a \equiv b \pmod{n}$, pak $b - a \equiv n \pmod{n}$.
- b) Nechť $n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$. Dokažte, že jestliže $a \equiv b \pmod{n^2}$, pak $a \equiv b \pmod{n}$.
- c) Nechť $n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$. Dokažte, že jestliže $a \equiv b \pmod{n}$, pak $2a + 3b \equiv 5b \pmod{n}$.
- d) Nechť $n \in \mathbb{N}$. Dokažte, že jestliže $a \in \mathbb{N}$, $a > 1$ dělí n , pak existuje $k \in \mathbb{N}$, $k < n$ takové, že $ak \equiv 0 \pmod{n}$.